Grover like Operator Using Only Single-Qubit Gates

G. Kato*
NTT Communication Science Laboratories,
NTT Corporation
3-1, Morinosato Wakamiya, Atsugi-shi,
Kanagawa Pref., 243-0198 Japan
(Dated: February 1, 2008)

We propose a new quantum circuit for the quantum search problem. The quantum circuit is superior to Grover's algorithm in some realistic cases. The reasons for the superiority are in short as follows: In the quantum circuit proposed in this paper, all the operators except for the oracle can be written as direct products of single-qubit gates. Such separable operators can be executed much faster than multi-particle operators, such as c-NOT gates and Toffoli gates, in many realistic systems. The idea of this quantum circuit is inspired by the Hamiltonian used in the adiabatic quantum computer. In addition, the scaling of the number of oracle calls for this circuit is the same as that for Grover's algorithm, i.e. $O\left(2^{n/2}\right)$.

PACS numbers: 03.67.Lx

I. INTRODUCTION

Since the concept of the quantum computer (QC) was proposed [1, 2, 3], many quantum algorithms [4, 5, 6, 7] that are superior to classical algorithms have been proposed. These algorithms have inspired many researchers, and the number of the researchers investigating the QC has increased dramatically as a result.

Though many results are generated daily, there remains a serious problem. The generated quantum circuits utilize the properties of quantum mechanics effectively, but almost all of then are modifications or combinations of just three quantum circuits based on quantum Fourier transformation [8], quantum amplitude amplification [9] or discrete quantum random walk [10]. This indicates that it is very hard to design new quantum circuits that use the properties of quantum mechanics effectively.

Recently, some frameworks differing from the QC have been proposed, such as the adiabatic quantum computer (AQC)[11], and the continuous random walk [12], and many results have been forthcoming in this area. In this paper, we focus on the AQC, whose procedure is identified by a Hamiltonian. Recently, it was proved that the calculation power of the AQC has the same as that of the QC [13]. This means that the QC can be emulated using the AQC and vice versa with polynomial time and space with respect to the input size. On the other hand, the properties of the problems that the QC and AQC are good at are different. These two facts indicate that new concepts of quantum circuits must be given by the explicit modification from the Hamiltonians for the AQC into finite size quantum circuits for the QC. We think this is a good strategy for designing new quantum circuits that use the properties of quantum mechanics effectively.

In this paper, we propose a new quantum circuit modified from a Hamiltonian for the AQC. This is the first simple example of a quantum circuit obtained by following the above strategy. Here, we treat the well-investigated problem in the QC, i.e., the quantum search problem, in order to check the efficiency of the strategy. As a result, we get a new quantum circuit that is superior to the quantum circuit used in Grover's algorithm in some cases. The Hamiltonian just gives us some hints, and the new quantum circuit is intuitively generated using those hints. Thus, we can not show some explicit procedures for the modification.

Here, we have to mention that, from the past work [14], quantum circuits for the QC can be easily modified from the Hamiltonians for the AQC, but the quantum circuits generated by the modification simply follow the time evolution of the AQC. Consequently, such quantum circuits are very redundant and inefficient for realistic calculations. The quantum circuits that we want to modify from the Hamiltonians are not such useless quantum circuits but practical ones.

To avoid any confusion, we should clarify that our circuit is superior in that it may be executed faster than Grover's algorithm in realistic systems since it uses only simple operators, each of which rotate just one-qubit, except for the oracle. However, the circuit does not offer reduced complexity. Actually, both it and Grover's algorithm have exactly the same complexity $O\left(2^{n/2}\right)$. For these reasons, the superiority of the new circuit will be meaningful mainly to experimentalists.

In Sec. II, we briefly review Grover's algorithm to facilitate comparison between it and the expressions for the new quantum circuit. In Sec. III, we show the explicit form of the new quantum circuit and prove that the quantum circuit can execute quantum search efficiently. In Sec. IV, we numerically simulate the new quantum circuit to show how well it executes quantum search. In Sec. V, we show the relations between quantum circuits and Hamiltonians for the AQC. These relations are the

*Electronic address: kato@theory.brl.ntt.co.jp

hints for generating the new quantum circuit. The last section summarizes our conclusions. Technical details of a proof are in Appendix A.

II. GROVER'S ALGORITHM

By Grover's algorithm, the quantum search problem can be solved. This means that we can find integer j from 0 to 2^n-1 using the oracle operator $\hat{O}_r$ such that

$$\hat{O}_r \left|m\right\rangle \otimes \left|k\right\rangle \ := \ \left|m\right\rangle \otimes \left|k \oplus \delta\left(m,j\right)\right\rangle \tag{1}$$

by the algorithm. The operator $\hat{O}_r$ acts on two registers: one is 2^n-dimensional, corresponding to the search space, and the other is 2-dimensional, corresponding to the output of the oracle. Grover's algorithm can be expressed as follows. First, we generate the initial state

$$\left|\bar{0}\right\rangle \ := \ 2^{-\frac{n}{2}} \sum_{m=0}^{2^n-1} \left|m\right\rangle . \tag{2}$$

Next, we iterate the two operations, which are identified by the following operator:

$$\hat{G} \ := \ 1 - 2\left|\bar{0}\right\rangle \left\langle\bar{0}\right| , \tag{3}$$

$$\hat{O} \ := \ 1 - 2\left|j\right\rangle \left\langle j\right| . \tag{4}$$

Note that, in general $\hat{G}\cdot\hat{O}$ is written by G, e.g., [15], and is called the Grover operator. The number of iterations is

$$N \ := \ \left[\frac{\pi}{4\arcsin 2^{-\frac{n}{2}}}\right], \tag{5}$$

where $[r]$ indicates the integer part of real number r. Note that the operator $\hat{O}$ (4) is outwardly different from the oracle operator $\hat{O}_r$ (1); however, $\hat{O}$ can be simulated from one use of $\hat{O}_r$ by using the second register as an ancilla prepared in state $\frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle$. Finally, we observe the state using the computational basis, i.e., $\left|0\right\rangle$, $\left|1\right\rangle$,$\cdots$,$\left|2^n-1\right\rangle$. The success probability of Grover's algorithm, i.e., the probability to detect the state $\left|j\right\rangle$, goes to 1 in the limit $n \to \infty$. This is equivalent to the following relation:

$$\lim_{n\to\infty} \left| \left\langle j\right| \left(\hat{G}\cdot\hat{O}\right)^N \left|\bar{0}\right\rangle \right|^2 \ = \ 1. \tag{6}$$

The scaling of the success probability versus n is $1 - O\left(2^{-n}\right)$. The relation (6) can be easily proved as follows.

Proof:

The operator $\hat{G}\cdot\hat{O}$ modifies any vector in the space spanned by $\left|\bar{0}\right\rangle$ and $\left|j\right\rangle$ into another vector in the same space. Then, we restrict the Hilbert space to the two dimensional space, i.e., $\{\left|\psi\right\rangle = a\left|\bar{0}\right\rangle + b\left|j\right\rangle\}$ in this proof. Under this restriction, the operator $\hat{G}\cdot\hat{O}$ can be written as the following two dimensional matrix:

$$\begin{aligned} \hat{G}\cdot\hat{O} \ &= \ -\begin{pmatrix} 1-2^{1-n} & -2^{1-\frac{n}{2}}\sqrt{1-2^{-n}} \\ 2^{1-\frac{n}{2}}\sqrt{1-2^{-n}} & 1-2^{1-n} \end{pmatrix} \\ &= \ -\begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}, \end{aligned} \tag{7}$$

$$\theta \ := \ \arcsin 2^{-\frac{n}{2}} \qquad 0 < \theta \le \frac{\pi}{2}. \tag{8}$$

Here, we use the basis $\left\{\left|\bar{0}\right\rangle, \left|\bar{1}\right\rangle := \frac{\left|j\right\rangle - 2^{-\frac{n}{2}}\left|\bar{0}\right\rangle}{\sqrt{1-2^{-n}}}\right\}$. From this expression, it is easy to show that

$$\begin{aligned} &\left| \left\langle j\right| \left(\hat{G}\cdot\hat{O}\right)^N \left|\bar{0}\right\rangle \right|^2 \\ &= \ \sin^2\left(2N+1\right)\theta \\ &= \ \sin^2\left(2\left[\frac{\pi}{4\arcsin 2^{-\frac{n}{2}}}\right]+1\right)\arcsin 2^{-\frac{n}{2}}. \end{aligned} \tag{9}$$

From the last equation, it is clear that relation (6) holds. □

III. QUANTUM SEARCH ALGORITHM USING A NEW QUANTUM CIRCUIT

A. The case of one solution

We propose a new quantum circuit by which the Grover iteration can be replaced.

The outline of the algorithm is the same as Grover's algorithm, but in order to avoid misunderstanding we show whole algorithm below. First, we prepare the initial state $\left|\bar{0}\right\rangle$, which is the same as the initial state of Grover's algorithm. Next, we iterate the two operations, which are identified by the following operator:

$$\hat{G}' \ := \ \exp\left(\varphi\left(\omega\right)\sum_{\alpha=0}^{n-1} S_x^{(\alpha)} i\right), \tag{10}$$

$$\hat{O}' \ := \ \exp\left(\omega\left|j\right\rangle\left\langle j\right| i\right). \tag{11}$$

The number of iterations is

$$N' \ := \ \left[\frac{\pi}{4\sin\left|\frac{\omega}{2}\right|}2^{\frac{n}{2}} + \frac{1}{2}\right]. \tag{12}$$

The variable ω in the above definition can be chosen from the region $-\pi < \omega < \pi$ and is independent of n and j. The operator $S_x^{(\alpha)}$ and the function $\varphi\left(\omega\right)$ are defined later. Finally, we observe the state using the computational basis. The success probability of this algorithm goes to 1 in the limit $n \to \infty$. This is equivalent to the following relation:

$$\lim_{n\to\infty} \left| \left\langle j\right| \left(\hat{G}'\cdot\hat{O}'\right)^{N'} \left|\bar{0}\right\rangle \right|^2 \ = \ 1. \tag{13}$$

The scaling of the success probability versus n is $1 - O\left(n^{-1}\right)$. A proof of relation (13) is located at the end of this section.

Here, we have to note three things. First, the scaling of the number of oracle calls is $O\left(2^{n/2}\right)$ for any $-\pi < \omega < \pi$ when $\omega \neq 0$. Here, we have to point out that the operator $\hat{O}'$ (11) can actually be simulated by a constant number of calls to the oracle $\hat{O}_r$ (1), where the number depends on ω. A method of simulation is as follows. We introduce a naturally generalized oracle as

$$\hat{O_r}' |m\rangle \otimes |k\rangle \ := \ |m\rangle \otimes |k + \delta(m,j) \mod \omega_d\rangle \quad (14)$$

for arbitrary integer ω_d. The operator $\hat{O_r}'$ (14) acts on two registers: one is 2^n-dimensional and the other is ω_d-dimensional. It is easy to show that this operator $\hat{O_r}'$ can be simulated by a constant number of calls to the oracle $\hat{O}_r$. Furthermore, the operator $\hat{O}'$ can be simulated from one use of $\hat{O_r}'$ by using the second register as ancillae prepared in state

$$\sum_{k=0}^{\omega_d - 1} \exp\left(\frac{k\omega_c}{\omega_d} 2\pi i\right) |k\rangle . \quad (15)$$

In this definition, ω_d and ω_c are chosen so as to satisfy $\frac{\omega_c}{\omega_d} 2\pi = \omega$. Then, the operator $\hat{O}'$ can be simulated by $\hat{O}_r$. Second, the difference in execution time between $\hat{O}_r$ and $\hat{O}'$ probably will not depend on n in most cases. This expectation comes form the following consideration. Once we know the explicit circuit for $\hat{O}_r$, we will probably be able to make a circuit corresponding to $\hat{O_r}'$ in such a way that the difference of execution time of these two circuits does not depend on n. This expectation has no meaning from a computer science point of view, since the oracle $\hat{O}_r$ is usually treated as a black-box. However, in case of actual calculations using a real system, it is important to think in term of the execution time of operations. Third, when $\omega = \pm\pi$, the relation (13) does not hold. This is related to the fact that the value ω influences not only the number of iterations N' but also the speed of the convergence (13). For example, when ω approaches $\pm\pi$, the speed of the convergence decreases. On the other hand, when ω approaches 0, the speed of the convergence increases. Here, the change in the speed means the change in the constant factor of the scaling.

Here, we define the function $\varphi(\omega)$ and the operator $S_x^{(\alpha)}$ used in the above outline of the algorithm. First, $S_x^{(\alpha)}$ is the operator which acts only on the α-th qubit, and the action on the qubit can be written as $\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$ using the computational basis. Therefore, we can write $S_x^{(\alpha)}$ as follows:

$$S_x^{(\alpha)} \ := \ Id \otimes \cdots \otimes \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \otimes \cdots \otimes Id. \quad (16)$$

Note that $2S_x^{(\alpha)}$ is simply Pauli operator σ_x applied on qubit α. Next, we define $\varphi(\omega)$ implicitly as follows:

$$\cot\frac{\omega}{2} \ = \ \sum_{s=1}^{n} P_n(s) \cot\frac{s\varphi(\omega)}{2},$$
$$-\frac{2\pi}{n} < \varphi(\omega) < \frac{2\pi}{n}, \quad \mathrm{sgn}(\omega) = \mathrm{sgn}(\varphi(\omega)) \quad (17)$$

where

$$P_n(s) \ := \ \frac{n! 2^{-n}}{s!(n-s)!}. \quad (18)$$

Recall that 2^n is the number of elements in the set from which item j is selected and that ω is an arbitrary number in the region $-\pi < \omega < \pi$. Note that the function $\varphi(\omega)$ depends on n. As an example, a plot of the function $\varphi(\omega)$ for $n = 10$ is shown in Fig 1.

The rest of this section is devoted to proving relation (13).

Proof:

First of all, we show the main idea underlying this proof in order to provide some insight into why it works. The idea consists of three parts. First, $\hat{G}'\hat{O}'$ leaves $\tilde{S}^2$ (19) eigenspaces invariant, and both $|\bar{0}\rangle$ and $|j\rangle$ lie in the same eigenspace, so we can restrict our study to this eigenspace. Second, $|\bar{0}\rangle$ and $|j\rangle$ have most of their support on the 2-dimensional subspace spanned by two particular eigenstates of $\hat{G}'\hat{O}'$, $|\psi_{\gamma_\pm}\rangle$ whose eigenvalues are $\gamma_\pm$ (28), so we can even more restrict our study to this subspace. Finally, due to the corresponding eigenvalues $\gamma_\pm$, we need to repeat $\hat{G}'\hat{O}'$ a certain number of times (12) to rotate $|\bar{0}\rangle$ to $|j\rangle$. Based on this idea, we obtain a strict proof as follows.

The operator $\hat{G}' \cdot \hat{O}'$ is a block diagonal matrix in the case of the computational basis and each block can be characterised by eigenvalues of the operator

$$\tilde{S}^2 := \left(\sum_{\alpha=0}^{n-1} S_x^{(\alpha)}\right)^2 + \left(\sum_{\alpha=0}^{n-1} \tilde{S}_y^{(\alpha)}\right)^2 + \left(\sum_{\alpha=0}^{n-1} \tilde{S}_z^{(\alpha)}\right)^2, \quad (19)$$

where

$$\tilde{S}_y^{(\alpha)} := (-)^{j^{(\alpha)}} Id \otimes \cdots \otimes \begin{pmatrix} 0 & -\frac{1}{2}i \\ \frac{1}{2}i & 0 \end{pmatrix} \otimes \cdots \otimes Id,$$
$$\tilde{S}_z^{(\alpha)} := (-)^{j^{(\alpha)}} Id \otimes \cdots \otimes \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} \otimes \cdots \otimes Id \quad (20)$$

and $j^{(\alpha)}$ is 0 or 1 such that

$$j \ = \ \sum_{\alpha=0}^{n-1} 2^\alpha j^{(\alpha)}. \quad (21)$$

Note that the operators $2\tilde{S}_y^{(\alpha)}$ and $2\tilde{S}_z^{(\alpha)}$ defined by (20) reduce to the Pauli operators in the special case j=0. Otherwise, the operators $2\tilde{S}_y^{(\alpha)}$ and $2\tilde{S}_z^{(\alpha)}$ are equivalent to the Pauli operators up to an overall phase. The states $|\bar{0}\rangle$ and $|j\rangle$ belong to the subspace whose eigenvalue for

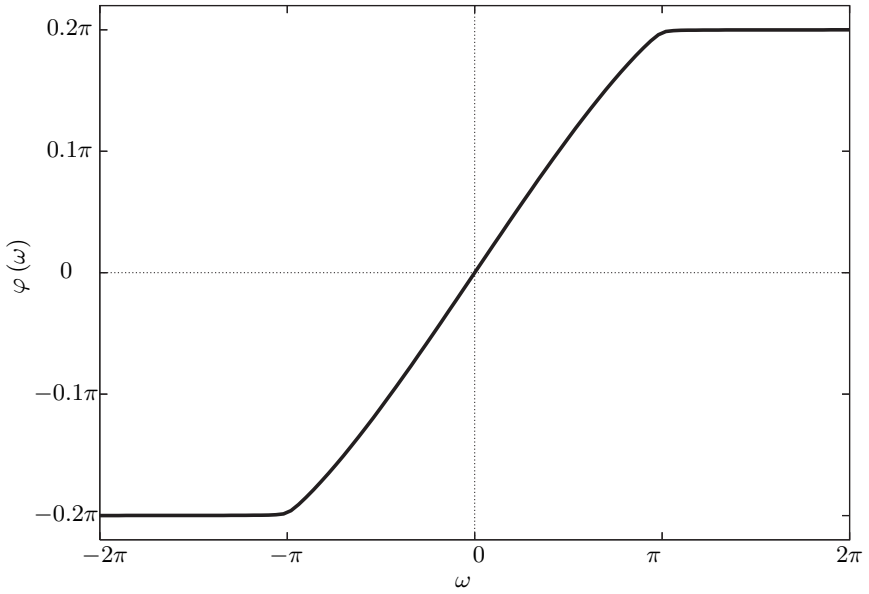

FIG. 1: A plot of the function $\varphi(\omega)$ defined by (17) for $n = 10$

$\tilde{S}^2$ is $n(n+2)/4$. This subspace reduces to the maximal total spin subspace in the special case $j = 0$. In the rest of this section, we restrict the Hilbert space to this subspace and use the following two bases

$$\left\{ |s_x\rangle \left| \sum_{\alpha=1}^{n} S_x^{(\alpha)} |s_x\rangle = (-s + n/2) |s_x\rangle \right. \right\}, \tag{22}$$

$$\left\{ |s_z\rangle \left| \sum_{\alpha=1}^{n} \tilde{S}_z^{(\alpha)} |s_z\rangle = (-s + n/2) |s_z\rangle \right. \right\}. \tag{23}$$

Note that it is easy to see that $|\bar{0}\rangle \propto |0_x\rangle$ and $|j\rangle \propto |0_z\rangle$. Then, over all phases are defined in such a way that $\langle s_x|0_z\rangle > 0$, $\langle 0_x|s_z\rangle > 0$, $|\bar{0}\rangle = |0_x\rangle$ and $|j\rangle = |0_z\rangle$.

The eigenvalues $\exp\left(\gamma + \frac{n\varphi(\omega)}{2}\right) i$ and the corresponding eigenvectors $|\psi_\gamma\rangle$ for $\hat{G}' \cdot \hat{O}'$ satisfy the relation

$$\frac{\langle s_x|\psi_\gamma\rangle}{1 - \exp(\omega i)} = \frac{\langle s_x|0_z\rangle \langle 0_z|\psi_\gamma\rangle}{1 - \exp(\gamma + s\varphi(\omega)) i}. \tag{24}$$

Then, the following two relations hold:

$$\frac{1}{1 - \exp(\omega i)} = \sum_{s=0}^{n} \frac{P_n(s)}{1 - \exp(\gamma + s\varphi(\omega)) i}, \tag{25}$$

$$\frac{1}{|1 - \exp(\omega i)|^2} = \sum_{s=0}^{n} \frac{P_n(s) |\langle 0_z|\psi_\gamma\rangle|^2}{|1 - \exp(\gamma + s\varphi(\omega)) i|^2}. \tag{26}$$

In the derivation of the above two relations, we use the relation

$$|\langle s_x|0_z\rangle|^2 = P_n(s). \tag{27}$$

Next, we show that there are two eigenvalue series $\exp\left(\gamma_\pm + \frac{n\varphi(\omega)}{2}\right) i$ for the operator $\hat{G}' \cdot \hat{O}'$ such that

$$\lim_{n\to\infty} 2^{\frac{n}{2}} \gamma_\pm = \pm 2 \sin\frac{\omega}{2}, \tag{28}$$

where we regard $\gamma_\pm$ as two series with respect to n defined by ω. In order to prove this relation, we use the following relation

$$\lim_{n\to\infty} \frac{n\varphi(\omega)}{2} = \omega. \tag{29}$$

Recall that the function $\varphi(\omega)$ is defined by (17). This relation is derived from

$$\lim_{n\to\infty} \sum_{s=1}^{n} P_n(s) \cot\frac{sr}{2n} = \cot\frac{r}{4}, \tag{30}$$

where $-2\pi < r < 2\pi$. Relation (30) is a special case of the following Lemma.

- *Lemma*:

$$\lim_{n\to\infty} \sum_{s=1}^{n} P_n(s) f\left(\frac{s}{n}\right) = f\left(\frac{1}{2}\right), \tag{31}$$

where $f(\zeta \in \mathbb{C})$ is a meromorphic function in the region $\left|\zeta - \frac{1}{2}\right| < 1/2 + \delta$ and has only one pole at point $\zeta = 0$.

(A proof of this lemma is given in Appendix A.) Then, relation (29) is proved. Now, we define two functions $g(n, \zeta)$ and $g^{(q)}(\zeta)$

$$g(n,\zeta) := \frac{1}{1 - \exp(\omega i)} - \sum_{s=0}^{n} \frac{P_n(s)}{1 - \exp(\zeta + s\varphi(\omega)) i}, \tag{32}$$

$$g^{(q)}(\zeta) := \frac{1}{q!} \frac{d^q}{d\tilde{\zeta}^q} \left. \frac{1}{1 - \exp\left(\tilde{\zeta} + \zeta\right) i} \right|_{\tilde{\zeta}=0}. \tag{33}$$

It is clear that $g(n,\gamma)$ is equal to 0 from condition (25). Then, the sufficient condition of (28),

$$\begin{aligned}
&\lim_{n\to\infty} g\left(n,\zeta 2^{-\frac{n}{2}}\right)2^{\frac{n}{2}} \\
&= \frac{1}{\zeta}i - \lim_{n\to\infty}\sum_{q=1}^{\infty}\sum_{s=1}^{n} P_n(s)\, g^{(q)}(s\varphi(\omega))\,\zeta^q 2^{-\frac{n(q-1)}{2}} \\
&= \frac{1}{\zeta}i - \sum_{q=1}^{\infty}\lim_{n\to\infty}\sum_{s=1}^{n} P_n(s)\, g^{(q)}(s\varphi(\omega))\,\zeta^q 2^{-\frac{n(q-1)}{2}} \\
&= \frac{1}{\zeta}i - \frac{\zeta}{4\sin^2\frac{\omega}{2}}i \qquad\qquad (34)\\
&\qquad\qquad \zeta\in\mathbb{C},\quad \zeta\neq 0,
\end{aligned}$$

is derived by using relation (29) and lemma (31). In the first equality, we make the Laurent expansion at $\zeta = 0$. In the second equality, we just exchange the order of the limit operations. In the last equality, we use relation (29) and lemma (31). Then, relation (28) is proved.

Next, we show the relations

$$\lim_{n\to\infty}\langle 0_z|\psi_{\gamma_\pm}\rangle\langle\psi_{\gamma_\pm}|0_x\rangle = \pm\frac{\exp\left(-\frac{\omega}{2}i\right)}{2}, \qquad (35)$$

$$\lim_{n\to\infty}\sum_{\gamma\neq\gamma_\pm}|\langle 0_x|\psi_\gamma\rangle|^2 = \lim_{n\to\infty}\sum_{\gamma\neq\gamma_\pm}|\langle 0_z|\psi_\gamma\rangle|^2 = 0, \qquad (36)$$

where $\sum_{\gamma\neq\gamma_\pm}$ means the summation with respect to all values γ corresponding to eigenvalues of $\hat{G}'\cdot\hat{O}'$ except for $\gamma_\pm$. From relation (26),

$$\begin{aligned}
&\lim_{n\to\infty}\left|\langle 0_z|\psi_{\gamma_\pm}\rangle\right|^{-2} \\
&= \lim_{n\to\infty}\sum_{s=0}^{n}\frac{P_n(s)\left|1-\exp(\omega i)\right|^2}{\left|1-\exp\left(\gamma_\pm + s\varphi(\omega)\right)i\right|^2} \\
&= 1 + \lim_{n\to\infty}\sum_{s=1}^{n}\frac{P_n(s)\left|1-\exp(\omega i)\right|^2}{\left|1-\exp\left(\gamma_\pm + s\varphi(\omega)\right)i\right|^2} \\
&= 2. \qquad (37)
\end{aligned}$$

In the second equality, we use (28), and in the third equality, we use (28), (29) and (31). On the other hand, from relation (24),

$$\begin{aligned}
\lim_{n\to\infty}\frac{\langle 0_z|\psi_{\gamma_\pm}\rangle}{\langle 0_x|\psi_{\gamma_\pm}\rangle} &= \lim_{n\to\infty}\frac{1-\exp(\gamma_\pm i)}{\langle 0_x|0_z\rangle\left(1-\exp(\omega i)\right)} \\
&= \pm\exp\left(-\frac{\omega}{2}i\right) \qquad (38)
\end{aligned}$$

is derived. Using relations (37) and (38), relation (35) is proved. Furthermore, from (37) and (38) and the trivial relation

$$\sum_\gamma|\langle 0_x|\psi_\gamma\rangle|^2 = \sum_\gamma|\langle 0_z|\psi_\gamma\rangle|^2 = 1, \qquad (39)$$

(36) is derived.

Using some relations proved above, we obtain

$$\begin{aligned}
&\lim_{n\to\infty}\left|\langle 0_z|\left(\hat{G}'\cdot\hat{O}'\right)^{N'}|0_x\rangle\right| \\
&= \lim_{n\to\infty}\left|\sum_\gamma\exp(N'\gamma i)\langle 0_z|\psi_\gamma\rangle\langle\psi_\gamma|0_x\rangle\right| \\
&= \lim_{n\to\infty}\left|\exp(N'\gamma_+ i)\langle 0_z|\psi_{\gamma_+}\rangle\langle\psi_{\gamma_+}|0_x\rangle\right. \\
&\qquad \left.+\exp(N'\gamma_- i)\langle 0_z|\psi_{\gamma_-}\rangle\langle\psi_{\gamma_-}|0_x\rangle\right| \\
&= \frac{1}{2}\lim_{n\to\infty}\left|\exp(N'\gamma_+ i)-\exp(N'\gamma_- i)\right| \\
&= 1. \qquad (40)
\end{aligned}$$

In the second equality, we use relation (36), in the third equality we use relation (35), and in the last one we use (28) and (12). Relation (40) is exactly the same as (13). □

B. The case of more than one solution

When there are two solutions, we also modify Grover's algorithm in the same way. However, we have to know humming distance d of the two solutions. This information is not used in Grover's algorithm. When we change the number of solutions, all we have to do is to change the definition of $\varphi(\omega)$ and N' as follows:

$$\begin{aligned}
\cot\frac{\omega}{2} &= \sum_{s_1=0}^{n-d}\sum_{s_2=\delta(s_1,0)}^{d}\left(1+(-)^{s_2}\right)P_{n-d}(s_1)\,P_d(s_2) \\
&\qquad\qquad \times\cot\frac{(s_1+s_2)\,\varphi_2(\omega)}{2}, \\
-\frac{2\pi}{n} &< \varphi_2(\omega) < \frac{2\pi}{n}, \quad \mathrm{sgn}(\omega) = \mathrm{sgn}\left(\varphi_2(\omega)\right), \qquad (41)
\end{aligned}$$

$$N_2' := \left[\frac{\pi}{4\sqrt{2}\sin\frac{\omega}{2}}2^{\frac{n}{2}}+\frac{1}{2}\right], \qquad (42)$$

where the subscript "2" of $\varphi(\omega)$ and N' indicates just the number of solutions. Then, the operator $\hat{G}'$ and the oracle $\hat{O}'$ become

$$\hat{G}_2' := \exp\left(\varphi_2(\omega)\sum_{\alpha=0}^{n-1}S_x^{(\alpha)}i\right), \qquad (43)$$

$$\hat{O}_2' := \exp\left(\omega\left(|j_1\rangle\langle j_1|+|j_2\rangle\langle j_2|\right)i\right). \qquad (44)$$

The success probability goes to 1 in the limit $n\to\infty$. This is equivalent to the following relation:

$$\lim_{n\to\infty}\sum_{\eta=1,2}\left|\langle j_\eta|\left(\hat{G}_2'\cdot\hat{O}_2'\right)^{N_2'}|\bar{0}\rangle\right|^2 = 1. \qquad (45)$$

We can prove this relation in the same way as we have done in the one solution case, so we omit it. We believe that the same relations hold when there are more than two solutions, and we numerically checked this fact in several cases.

IV. NUMERICAL CALCULATION

In order to check that the new quantum circuit works well, we numerically calculated the iteration number, i.e., N' defined by (12), and the error rate, i.e., $1-\left|\langle j|\left(\hat{G}'\cdot\hat{O}'\right)^{N'}|\bar{0}\rangle\right|^2$, at $n=10,20,30,40$ and $\omega=\frac{\pi}{2},\frac{2\pi}{3},\frac{3\pi}{4},\frac{4\pi}{5},\pi$. The results are shown in Table I. In order to compare the proposed quantum circuit with the quantum circuit used in Grover's algorithm, we also show the corresponding values for Grover's algorithm in the table. Note that, N' and $\varphi(\omega)$ when $\omega=\pi$ are defined in the same way as the other four example, i.e. (12) and (17).

From the result when $\omega=\pi$, we predict that the relation

$$\lim_{n_o\to\infty}\inf_{n_0<n}\left|\langle j|\left(\hat{G}'\cdot\hat{O}'\right)^{N'}|\bar{0}\rangle\right|^2 = Const \qquad 0<Const<1 \tag{46}$$

holds when case $\omega=\pi$. This relation may be proved in a way similar to that in the other ω case. This relation means that we can probably use the quantum circuit, i.e. $\left(\hat{G}'\cdot\hat{O}'\right)^{N'}$, for the quantum search problem even when $\omega=\pi$, though the error rate for the circuit will be much bigger than that in other ω cases.

What we want to mention about the results for the cases $\omega=\frac{\pi}{2},\frac{2\pi}{3},\frac{3\pi}{4},\frac{4\pi}{5}$ is that the error rate is sufficiently small for realistic n cases. On the other hand, it is fair to point out that with the algorithm using the new quantum circuit, the number of iterations and the error rate are much higher than in Grover's algorithm. However, the results do not provide enough information for us to discuss the efficiency of the two algorithms. We remark that operator $\hat{G}$ is a really multi-particle operator, whereas operator $\hat{G}'$ is just a set of single-particle rotation, i.e., a direct product of single-qubit operators. The "really multi-particle operators" are those that can not be expressed only by products of single-qubit operators. Therefore, operator $\hat{G}'$ can be executed much faster than $\hat{G}$ in many realistic systems. Then, the average time to find solution j by the algorithm using the new quantum circuit is shorter than that by Grover's algorithm in some cases on a realistic QC.

V. RELATION BETWEEN THE PROPOSED QUANTUM CIRCUIT AND THE AQC

The quantum circuit proposed in this paper is inspired by Farhi's Hamiltonian [11] for the AQC. In this section, we briefly review the AQC, point out the simple relation between the quantum circuit used in Grover's algorithm and Roland's Hamiltonian [16] for quantum search on the AQC, and finally point out the similar relation between the proposed quantum circuit and Farhi's Hamiltonian for quantum search on the AQC. Recall that to generate a new quantum circuit, we assumed the existence of operator $\hat{G}'$ related to Farhi's Hamiltonian as an analogy of the relation between the Grover operator and Roland's Hamiltonian. This relation is shown below. Then, we find the explicit expression of operator $\hat{G}'$, i.e., (10).

The AQC involve the following procedures. First, we define the parametrised hermitian matrix $\hat{H}(r)$ that has the following five properties.

- The operator $\hat{H}(r)$ is continuously changed with respect to parameter $r\in\mathbb{R}$.
- The ground state of $\hat{H}(0)$ is a simple general state.
- The ground state of $\hat{H}(1)$ is an encoded solution of the problem.
- At any $0\le r\le 1$, the ground state of $\hat{H}(r)$ does not degenerate.
- The Hamiltonian can be easily defined using only the definition of the problem, i.e., the Hamiltonian can be defined without knowing the result.

Second, we prepare the initial state that is the ground state of $\hat{H}(0)$. Third, we make the time evolution of the state such that

$$i\frac{\partial}{\partial t}|\phi_T(t)\rangle = \hat{H}\left(\mu\left(\frac{t}{T}\right)\right)|\phi_T(t)\rangle$$
$$\mu(0)=0 \quad \mu(1)=1 \quad \frac{d}{dr}\mu(r)>0. \tag{47}$$

Note that $\mu(r)$ can be chosen arbitrarily until the above conditions are satisfied, but the choice affects the probability of success and the time for the calculation. Finally, we observe the state at time $t=T$. If T is sufficiently large, the correct solution is obtained, i.e.,

$$\lim_{T\to\infty}|\langle\phi_g(r)|\phi_T(rT)\rangle| = 1 \tag{48}$$

where $|\phi_g(r)\rangle$ is a ground state of the operator $\hat{H}(r)$. A suitable value of T can be found from the adiabatic theorem. This is a rough sketch of the AQC.

Next, we show the relation between the quantum circuit used in Grover's algorithm and Roland's Hamiltonian for quantum search [16] on the AQC. The Hamiltonian

$$\hat{H}_R(r) := -(1-r)|\bar{0}\rangle\langle\bar{0}| - r|j\rangle\langle j| \tag{49}$$
$$\mu_R(r) := \frac{\sin(\pi-2\theta)r}{\sin(\pi-2\theta)r+\sin((\pi-2\theta)r+2\theta)} \tag{50}$$

executes quantum search, where $|\bar{0}\rangle$ and θ mean the same state and value as those in the previous section, i.e., (2) and (8), and j is the target of the search. The above function $\mu_R(r)$ is optimised so as to maximize the success

# of items, i.e., 2^n	Grover	$\omega = \frac{\pi}{2}$	$\omega = \frac{2\pi}{3}$	$\omega = \frac{3\pi}{4}$	$\omega = \frac{4\pi}{5}$	$\omega = 1$
2^{10}	25	36	29	27	26	25
	5.4×10^{-4}	2.2×10^{-1}	2.5×10^{-1}	2.7×10^{-1}	2.9×10^{-1}	6.8×10^{-1}
2^{20}	804	1137	929	871	846	804
	2.4×10^{-7}	8.5×10^{-2}	9.7×10^{-2}	1.1×10^{-1}	1.1×10^{-1}	6.2×10^{-1}
2^{30}	25735	36396	29717	27856	27060	25736
	6.8×10^{-10}	5.0×10^{-2}	5.8×10^{-2}	6.3×10^{-2}	6.8×10^{-2}	6.1×10^{-1}
2^{40}	823549	1164675	950953	891404	865931	823550
	9.8×10^{-14}	3.5×10^{-2}	4.1×10^{-2}	4.5×10^{-2}	4.9×10^{-2}	6.0×10^{-1}

TABLE I: The upper integer in each cell indicates the optimal iteration number, i.e., N or N'. The lower real number in each cell indicates the error rate, i.e., $1 - \left|\langle j| \left(\hat{G}\cdot\hat{O}\right)^N |\bar{0}\rangle\right|^2$ or $1 - \left|\langle j| \left(\hat{G}'\cdot\hat{O}'\right)^N |\bar{0}\rangle\right|^2$. The optimal iteration number and error rate in the case of Grover's algorithm are in the leftmost column, and those for the algorithm using the proposed quantum circuit at $\omega = \frac{1}{2}\pi, \frac{2}{3}\pi, \frac{3}{4}\pi, \frac{4}{5}\pi, \pi$ are in the other columns. Note that, N' and $\varphi(\omega)$ when $\omega = \pi$ are defined in the same way as the other four examples, i.e. (12) and (17). However, as pointed out in sec. III, relation (13) does not hold in that case. All the values were calculated for the case of only one solution.

probability. From this expression, it is readily known that

$$\begin{aligned} \hat{G} &= \exp\left(i\pi 2\left(1-\mu_R^*\right)\hat{H}(0)\right) \\ \hat{O} &= \exp\left(i\pi 2\mu_R^*\hat{H}(1)\right), \end{aligned} \tag{51}$$

where the operators $\hat{G}$ and $\hat{O}$ are defined by (4) and μ_R^* satisfies the condition that the gap between the two lowest eigenvalues of $\hat{H}_R(r)$ becomes the minimum value at the point $r = \mu_R^*$. Furthermore, by some calculations, we can check that

$$\lim_{T\to\infty}\left|\left\langle \phi_T\left(\frac{4\theta T}{\pi-2\theta}m\right)\right|\left(\hat{G}\cdot\hat{O}\right)^m|\bar{0}\rangle\right| = 1 \tag{52}$$

where $0 \le m \le \left[\frac{\pi}{4\theta}+\frac{1}{4}\right]$ is an integer. This relation means that the optimal speed of an AQC using Roland's Hamiltonian is exactly the same as the speed of Grover's algorithm with respect to quantum search.

Next, we show the relation between the quantum circuit proposed in this paper and Farhi's Hamiltonian [11] for quantum search on an AQC. The Hamiltonian

$$\hat{H}_F(r) := -(1-r)\sum_{\alpha=0}^{n-1} S_x^{(\alpha)} - r|j\rangle\langle j| \tag{53}$$

also executes quantum search. As is easily shown, the following relation holds

$$\begin{aligned} \hat{G}' &= \exp\left(i\pi\xi\left(1-\mu_F^*\right)\hat{H}_F(0)\right) \\ \hat{O}' &= \exp\left(i\pi\xi\mu_F^*\hat{H}_F(1)\right), \end{aligned} \tag{54}$$

where $\xi := \omega/\mu_F^*$ is a real number. Relations (51) and (54) are very similar. However, we can only check that the leading term of μ_F^* as a function of n is the same as that of $\mu_F^{*\prime}$, where at the point $r = \mu_F^{*'}$ the gap between the two lowest eigenvalues of $\hat{H}_F(r)$ becomes the minimum value. Unfortunately, we have not yet found a relation like (52) in this case.

What we want to say in this section is that there are some relations between the quantum circuits for the QC and the Hamiltonians for the AQC, and these relations can be used to generate new quantum circuits. Some people may think that these relations are trivial or just accidental things. However, it is a truth that the proposed quantum circuit is found on the basis of the conviction that there must be an operator $\hat{G}'$ related to (53) as an analogy of the relation between $\hat{G}$ and (49), i.e., (51) and (52). Accordingly, we believe that there are more hidden relations between quantum circuits and Hamiltonians and that they would be powerful instruments for generating new quantum circuits and new Hamiltonians.

VI. CONCLUSION

We have proposed a new quantum circuit for the quantum search problem. This quantum circuit is superior to the quantum circuit used in Grover's algorithm in some cases on a realistic quantum computer. The reasons for this superiority in short are as follows: In the quantum circuit proposed in this paper, all the operators except for the oracle are direct products of single-qubit gates. In the quantum circuit used in Grover's algorithm, there are the operators other than the oracle, which are really multi-particle operators. On the other hand, it is a fact that the product of single-qubit gates can be executed much faster than multi-particle operators in many realistic systems. In addition, the scaling of the number of oracle calls for this circuit is the same as that for Grover's algorithm, i.e. $O\left(2^{n/2}\right)$.

The proposed circuit is found by a comparison of circuits for the quantum computer and Hamiltonian for the adiabatic quantum computer. This fact indicates that the comparison is probably one of the powerful instru-

ments for finding efficient new quantum circuits.

One aspect of future work is to find a stricter relation between the quantum circuits for the quantum computer and the Hamiltonians for the adiabatic quantum computer that gives sufficient data for modification from the Hamiltonians into the quantum circuits. Then, we will be able to automatically generate other efficient quantum circuits from Hamiltonians for the adiabatic quantum computer with respect to other problems that the adiabatic quantum computer is good at and discover new concepts for quantum circuits.

acknowledgements

The author wish to thank Y. Kawano, S. Tani, Y. Takahashi and Y. Nakajima for discussions and valuable comments.

APPENDIX A: PROOF OF LEMMA (31)

Here, we prove lemma (31).

Proof:

The sufficient condition of (31) is the relation

$$\lim_{n\to\infty}\sum_{s=1}^{n} P_n(s)\left(\frac{s}{n}\right)^q = 2^{-q}$$

$$q \in \mathbb{Z}, \tag{A1}$$

We can check this as follows:

$$\begin{aligned}
&\lim_{n\to\infty}\sum_{s=1}^{n} P_n(s) f\left(\frac{s}{n}\right)\\
=\ &\lim_{n\to\infty}\sum_{s=1}^{n} P_n(s)\left(\sum_{q=-\alpha}^{-1}\left(\frac{s}{n}\right)^q f^{(q)} + \sum_{q=0}^{\infty}\left(\frac{s}{n}-\frac{1}{2}\right)^q f^{(q)}\right)\\
=\ &\sum_{q=-\lambda}^{-1} f^{(q)} \lim_{n\to\infty}\sum_{s=1}^{n} P_n(s)\left(\frac{s}{n}\right)^q + \sum_{q=0}^{\infty} f^{(q)} \lim_{n\to\infty}\sum_{s=1}^{n} P_n(s)\left(\frac{s}{n}-\frac{1}{2}\right)^q\\
=\ &\sum_{q=-\lambda}^{-1} f^{(q)} 2^{-q} + f^{(0)}\\
=\ &f\left(\frac{1}{2}\right),
\end{aligned} \tag{A2}$$

where $f^{(q)}$ is defined as

$$f(\zeta) = \sum_{q=-\lambda}^{-1}\zeta^q f^{(q)} + \sum_{q=0}^{\infty}\left(\zeta-\frac{1}{2}\right)^q f^{(q)}. \tag{A3}$$

The (A1) is used in the third equality. The other equalities are easily given from the above definition of $f^{(q)}$

In the rest of this appendix, we prove relation (A1). We define some functions,

$$F(n,q) := \sum_{s=1}^{n} P_n(s)\left(\frac{s}{n}\right)^q \tag{A4}$$

$$n^q\tilde{F}(n,q) := \sum_{s=\max(q,1)}^{n}\frac{s!}{(s-q)!}P_n(s), \tag{A5}$$

$$= \begin{cases} \frac{n!2^{-q}}{(n-q)!} & \text{in case of } q>0\\ \frac{n!2^{-q}}{(n-q)!} - \sum_{s=q}^{0}\frac{n!2^{-n}}{(s-q)!(n-s)!} & \text{in case of } q\le 0. \end{cases} \tag{A6}$$

From these definitions, we can derive the relation

$$\begin{aligned}
&\tilde{F}(n,q)\\
\le\ &F(n,q)\\
\le\ &\left(\frac{n}{n-4q}\right)^q\tilde{F}(n,q) + \sum_{s=1}^{\left[\frac{n}{4}\right]+1} P_n(s)\left(\frac{s}{n}\right)^q.
\end{aligned} \tag{A7}$$

for $n > 4q$. Using the following relation

$$\lim_{n\to\infty} n!\frac{e^n}{n^{n+\frac{1}{2}}\sqrt{2\pi}} = 1, \tag{A8}$$

we can see that both the upper bound and the lower bound of $F(n,q)$ goes to 2^{-q} in the limit $n\to\infty$. □

[1] P. Benioff, J. Stat. Phys. **29**(1982)515.

[2] D. Deutsch, Proc. R. Soc. Lond. **A400**(1985)97.

[3] R. P. Feynman, Optic News, **11**(1985)11.
[4] D. Deutschand and Jozsa, Proc. R. Soc. Lond. **A439**(1992)553.
[5] P. Shor, *in Proc. 35th Annu. Symp. on the Foundations of Computer Science* (1994)124.
[6] L. K. Grover, Phys. Rev. Lett. **79**(1997)325.
[7] S. Tani, H. Kobayashi and K. Matsumoto *in Proc. 22nd Annu. Symp. on Theoretical Aspects of Computer Science*(2005)581.
[8] A. Yu Kitaev, quant-ph/9511026.
[9] G. Brassard, P. Høyer, M. Mosca and A. Tapp, quant-ph/0005055.
[10] D. Aharanov, A. Ambainis, J. Kempe and U. Vazirani, *Proc. 33rd Annu. Symp. on Theory of Computing,*(2001)50.
[11] E. Farhi, J. Goldstone, S. Gutmann and M. Sipser, quant-ph/0001106.
[12] E. Farhi and S. Gutmann, Phys. Rev. A **58**(1998)915, quant-ph/9706062.
[13] D. Aharonov, W. Dam, J. Kempe, Z. Landau and S. Lloyd, quant-ph/0405098.
[14] S. Lloyd, Science **273**(1996)1073.
[15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[16] J. Roland and N.J. Cerf, Phys. Rev. A **65**(2002)042308, quant-ph/0107015.